Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Vitor Magalhães de Oliveira

Tecnologia PowerLine:

Transmitindo Voz e Dados Através da Rede Elétrica

Rio de Janeiro

2010

Vitor Magalhães de Oliveira

Tecnologia PowerLine:

Transmitindo Voz e Dados Através da Rede Elétrica

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

Rio de Janeiro

2010

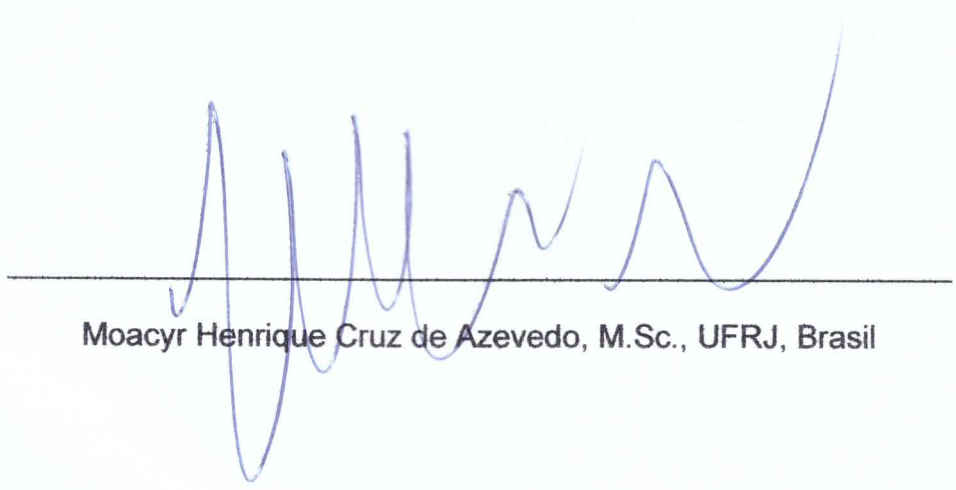
Vitor Magalhães de Oliveira

Tecnologia PowerLine:

Transmitindo Voz e Dados Através da Rede Elétrica

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em maio de 2010.



Moacyr Henrique Cruz de Azevedo, M.Sc., UFRJ, Brasil

AGRADECIMENTOS

Agradeço ao meu pai pelo apoio, incentivo e por acordar mais cedo pra me levar no ponto de ônibus, agradeço à minha mãe pela força me dada ao longo do curso, às minhas irmãs por liberarem o computador pra eu fazer meus trabalhos e minha monografia.

Agradeço aos meus colegas de curso por fazerem com que o curso ficasse mais agradável e divertido, aos funcionários do NCE por sempre nos atenderem com muita boa vontade, e ao meu coordenador Moacyr por ficar me cobrando e me lembrando sempre que o prazo estava acabando para que eu pudesse entregar minha monografia.

Agradeço também ao Larry Page e Sergey Brin por fundarem essa maravilhosa ferramenta de pesquisa que muito me auxiliou ao longo do curso e também para a realização da monografia.

RESUMO

OLIVEIRA, Vitor Magalhães de. **TECNOLOGIA POWERLINE: Transmitindo Voz e Dados Através da Rede Elétrica**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2010.

Este trabalho explica o funcionamento da Tecnologia PLC, que foi desenvolvida com o objetivo de tornar possível a transmissão de informações (dados e voz) usando como meio físico a infraestrutura já existente de cabeamento da rede elétrica.

Serão apresentadas as tecnologias que tornam possível esse tipo de transmissão; o histórico dessas tecnologias explicando como elas foram criadas; em que se basearam; a evolução das mesmas ao longo dos anos; funcionalidades e aplicações dessa tecnologia; e as vantagens e desvantagens de seu uso para o envio de dados através de uma rede local (LAN), e por uma conexão banda larga.

Outro ponto que também é analisado é a forma como ela foi regulamentada pela Anatel e pela ANEEL, mostrando a escolha dos padrões adotados para essa tecnologia no Brasil.

ABSTRACT

OLIVEIRA, Vitor de Magalhaes. POWERLINE TECHNOLOGY: Transmitting voice and data over power lines. Monograph (Specialization in Network Management and Internet Technology). Electronic Computer Center, Federal University of Rio de Janeiro. Rio de Janeiro, 2010.

This paper explains the function of PLC technology, which was developed with the aim of making possible the transmission of information (data and voice) utilizing the physical infrastructure of existing electrical cabling.

Will present the technologies that make possible this type of transmission; the history of these technologies by explaining how they were created; on which they relied to their evolution over the years; features and applications of this technology; and the advantages and disadvantages of their use for sending data over a local area network (LAN), and a broadband connection.

What also which is examined is how it was regulated by the ANATEL and ANEEL, showing the choice of setting standards for this technology in Brazil.

LISTA DE FIGURAS

	Página
Figura 1 - Esquema de funcionamento do Power Line Carrier	15
Figura 2 - Ligação de esquemas Power Line carrier através de modems	16
Figura 3 - Modulação FSK	19
Figura 4 - Modulação OFDM	19
Figura 5 - Esquema de transmissão CSMA	21
Figura 6: Algoritmo de Criptografia DES	23
Figura 7 - Exemplo de uma rede PLC em soluções residenciais.	25
Figura 8 - Exemplo de uma rede de serviços de uma concessionária	26
Figura 9 - Dispositivo Passport	28
Figura 10 - Dispositivo PowerPacket	30
Figura 11 - Equipamento HD_PLC	32
Figura 12 - Exemplo de formato longo de quadro	34
Figura 13 - Redes Lógicas Homeplug	42
Figura 14 - Funcionamento de uma rede BPL	45

LISTA DE TABELAS

	Página
Tabela 1 - Informações sobre controle de quadros	36
Tabela 2 - Recomendações sobre prioridade para o Homeplug	37
Tabela 3 - Throughput da Camada Física com diferentes Modulações e FEC	39
Tabela 4 - Throuput de Diferentes Camadas	40
Tabela 5 - Comparação de Throughput entre o Homeplug e outras tecnologias	40
Tabela 6 - Exemplo de uma tabela de chaves de criptografia	41
Tabela 7 - Limites de radiações indesejadas causadas por sistemas BPL de RBT	46
Tabela 8 - Limites de radiações indesejadas causadas por sistemas BPL de RMT	47
Tabela 9 - Faixas de freqüências em redes de média tensão excluídas	47
Tabela 10 - Faixas de Radiofreqüências relativas à zona de proteção de estações costeiras	48
Tabela 11 - Coordenadas das Zonas de Proteção de Estações Costeiras	49

LISTA DE SIGLAS

ACK / NACK – Sinais eletrônicos de reconhecimento usado em transmissões de dados
AES – Padrão de Criptografia Avançado
ANATEL – Agência Nacional de Telecomunicações
ANNEL – Agência Nacional de Energia Elétrica
APTEL - Associação de Empresas Proprietárias de Infra-Estrutura e de Sistema Privados de Telecomunicações
ASCII – Codificação de caracteres de 7 bits
BB – Bobina de Bloqueio
BPL – Rede de distribuição de banda larga através da Rede Elétrica
CAP – Prioridade de acesso ao canal
CSMA/CA - Sensor de portadora de múltiplo acesso com prevenção de colisões
DBPSK – Tipo de modulação
DEK – Padrão de Criptografia de Chaves
DES – Padrão de criptografia de dados
DIFS – Instante de tempo que uma estação aguarda quando deseja transmitir
DQPSK – Tipo de modulação
DSL – Conjunto de tecnologias que fornecem um meio de transmissão digital através da rede de telefonia
EKS – Seleção de Chaves de Criptografia
EOF – Delimitador de fim do quadro
ETHERNET – Tecnologia que define o tipo de cabeamento, sinais elétricos, formato de pacotes e protocolos, para interconexão de redes.
FCC - Agência Regulatória Federal de Serviços de Telecomunicações
FCS – Sequência de verificação dos quadros
FEC – Técnica de correção antecipada de erros
FSK - Modulação por chaveamento de frequência
Gbps, Mbps, Kbps – Unidades de medida que determinam a velocidade de uma comunicação
Hz, kHz GHz – Unidades de medida de Frequência
IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos
IP – Endereço de um equipamento em uma rede de comunicação
kV – Unida de medida de Tensão
LAN – Rede local de comunicação de dados
MAC – endereço físico da interface de rede
NEK – Chave de Criptografia de Rede
NIST – Instituto Americano Nacional de Padrões de Tecnologias
OFDM – Modulação por divisão ortogonal de frequência
OPLAT – Ondas Portadores em Linhas de Alta Tensão
PAYLOAD – Carga útil do pacote
PCI – É um elemento para interconectar periféricos em computadores
PCS – Sentido físico da portadora
PLC – Método de comunicação de dados através da Rede Elétrica
PLTF – Fórum sobre Comunicações PLC
PRS – Slots de resolução prioritária

QoS – Qualidade de serviço
RBT – Redes de baixa tensão
RMT – Redes de média tensão
RS-232 – Padrão para troca serial de dados binários
SOF – Delimitador de início do quadro
TCP/IP – Conjunto de protocolos de comunicação entre computadores em rede
TDMA – Acesso múltiplo por divisão de tempo
THROUGHPUT – Taxa de transferência da rede
TPC – Transformador de Potencial Capacitivo
USB – Tipo de conexão que permite a conexão de periféricos sem a necessidade de desligar o computador
UTP – Cabo par trançado sem blindagem
VCS – Sentido virtual da portadora
VLAN – Rede local virtual
VoIP – Tecnologia de transmissão de voz através de rede de dados

SUMÁRIO

	Página
1 - INTRODUÇÃO	12
2 - CONHECENDO A TECNOLOGIA PLC	14
2.1 - HISTÓRICO	14
2.2 - BASES TECNOLÓGICAS	18
2.2.1 - Modulações	18
2.2.1.1 - Modulação por Chaveamento de Freqüência	18
2.2.1.2 - Modulação por Divisão Ortogonal de Freqüência	19
2.2.2 - Métodos de Transmissão CSMA / CA	20
2.2.3 - Métodos de Criptografia	21
2.2.3.1 - Padrão de Criptografia de Dados	22
2.2.3.2 - Padrão de Criptografia Avançada	23
2.3 - APLICAÇÕES E SERVIÇOS OFERECIDOS	25
2.3.1 - Aplicações Residenciais e SOHO	25
2.2.2 - Serviços Oferecidos	26
3 - TECNOLOGIAS PLC INDOOR	27
3.1 - TECNOLOGIA PASSAPORT	28
3.2 - TECNOLOGIA POWERPACKET	29
3.3 - TECNOLOGIA HD-PLC	31
3.4 - TECNOLOGIA HOMEPLUG	32
4 - TECNOLOGIA HOMEPLUG	33
4.1 - CAMADA FÍSICA	33
4.2 - FORMATO DOS QUADROS	34
4.3 - MECANISMO DE ACESSO	35
4.4 - MECANISMOS DE SEGMENTAÇÃO E REMONTAGEM	38
4.5 - RECURSOS DE QoS	38
4.6 - PERFORMANCE	39
4.7 - SEGURANÇA	40
4.8 - TESTES DE CAMPO	43
5 - PLC OUTDOOR (BPL)	44
5.1 - FUNCIONAMENTO DE UMA REDE BPL	44
5.2 - CONDIÇÕES DE USO DE RADIOFREQUÊNCIAS BPL	46
5.3 - MONITORAMENTO DE ENERGIA ATRAVÉS DO BPL	50
6 - CONCLUSÃO	52
7 - REFERÊNCIAS BIBLIOGRÁFICAS	53

1 INTRODUÇÃO

Nos últimos anos muito tem se falado sobre “inclusão digital”, que é, basicamente, trazer um maior acesso à tecnologia para aqueles indivíduos que não possuem esse tipo de conhecimento a fim de tornar essas pessoas mais capazes a realizarem tarefas comuns, tais como trocas de e-mails, transações bancárias, pesquisas estudantis, compra e venda de produtos, etc, de uma forma rápida e prática.

A cada ano, devido à constante necessidade de mais pessoas estarem conectadas, a demanda por acesso à internet via banda larga é cada vez maior, pois um maior número de pessoas precisam se conectar de uma forma mais simples, rápida e barata. Esse aumento de pessoas conectadas é de grande interesse dos Governos Federal, Estaduais e Municipais, que em parceria com diversas empresas já promovem campanhas de inclusão digital em várias regiões do país, principalmente regiões onde o acesso à informação é mais difícil, como no interior dos Estados. Assim, vemos o quanto a inclusão digital tem mudado a vida de muitas pessoas, e diversas regiões, trazendo desenvolvimento, informação, especialização e emprego para essas localidades.

Hoje em dia não temos como falar de inclusão digital sem falar do acesso à internet por banda larga, por isso vem sendo estudadas várias formas de acesso à rede por banda larga de um modo mais abrangente, atingindo principalmente regiões mais afastadas dos grandes centros industriais e comerciais, e também com um custo cada vez mais reduzido.

Uma das grandes apostas dessas novas tecnologias, são as redes PLC (PowerLine Communications), que pelo fato de consistirem basicamente no tráfego de informações através de uma estrutura de cabeamento já existente da rede elétrica de

baixa e média tensão, e por essa infra-estrutura já estar pronta em mais de 90% do território nacional, tem se tornado uma proposta bastante atraente para levar banda larga aos locais onde não existem ainda estrutura montada para acesso à internet de forma rápida. Além da vantagem da infra-estrutura dos meios de acesso já estarem prontos, não havendo custo e nem trabalho para montar toda essa estrutura.

O grande problema seria como fazer com que dados e corrente elétrica caminhem juntos através do mesmo meio físico de transmissão. Como isso seria possível, pois sabe-se que a eletricidade causa diversas interferências em redes e não é aconselhável passar juntos em um mesmo eletroduto um cabo UTP de rede e um cabo elétrico.

A resposta para essa questão é que as redes PLC operam com uma faixa de frequência dos sinais muito diferentes da faixa de sinais usados pela energia elétrica (a energia elétrica trafega na faixa do Hz enquanto os dados via PLC trafegam na faixa do MHz), permitindo que eles possam conviver no mesmo meio físico sem grandes problemas, alcançando taxas de até 200Mbps para redes locais(LAN´s).

Essa tecnologia também pode ser utilizada como uma rede Metropolitana, para fornecer serviços, por exemplo, de um provedor de internet banda larga. A tecnologia que torna possível esse tipo de serviço é chamada BPL (Broadband over Powerlines).

2 CONHECENDO A TECNOLOGIA PLC

2.1 HISTÓRICO

A tecnologia PLC foi desenvolvida a partir de uma tecnologia já existente desde a década de 1920, tecnologia essa chamada de Power Line Carrier. O grande objetivo da criação desta tecnologia era fornecer meios para que as concessionárias de energia elétrica pudessem realizar serviços de comunicação de dados entre suas máquinas. Na época essa comunicação era feita em baixa velocidade, com velocidades de transmissão que não passavam de 9,6 Kbps. Podemos usar também como exemplo para este tipo de comunicação: telemetria, controle / comando de reatores na rede de baixa tensão, e comunicações de voz.

No Brasil essa tecnologia também era conhecida como OPLAT (Ondas Portadoras em Linhas de Alta Tensão).

O Power Line Carrier, ou OPLAT, trabalha utilizando modulação analógica, com uma baixa faixa de frequência entre 30 kHz e 400 kHz, e com as faixas de tensões entre 69 kV e 500 kV.

Para um melhor entendimento do funcionamento da tecnologia Power Line Carrier, a figura 1 mostra de uma forma resumida como essa tecnologia é utilizada dentro das subestações de energia.

Um Transformador de Potencial Capacitivo (TPC) é responsável por inserir e retirar sinais de alta frequência na rede elétrica de alta tensão. Esse transformador é instalado na chegada da linha de transmissão e também tem a função de trabalhar como um filtro para tratar apenas de sinais de alta frequência (maiores do que 100Khz). Ele é conectado antes de uma Bobina de Bloqueio (BB), sendo instalado na entrada da subestação A, tendo por finalidade filtrar as frequências altas e permitir que apenas

frequências menores do que 600 Khz possam chegar ao transformador. Essa combinação faz com que os sinais de elétrica e de dados sigam caminhos diferentes na entrada da subestação, pois eles estão trafegando no mesmo meio físico mas com faixas de frequências totalmente diferentes.

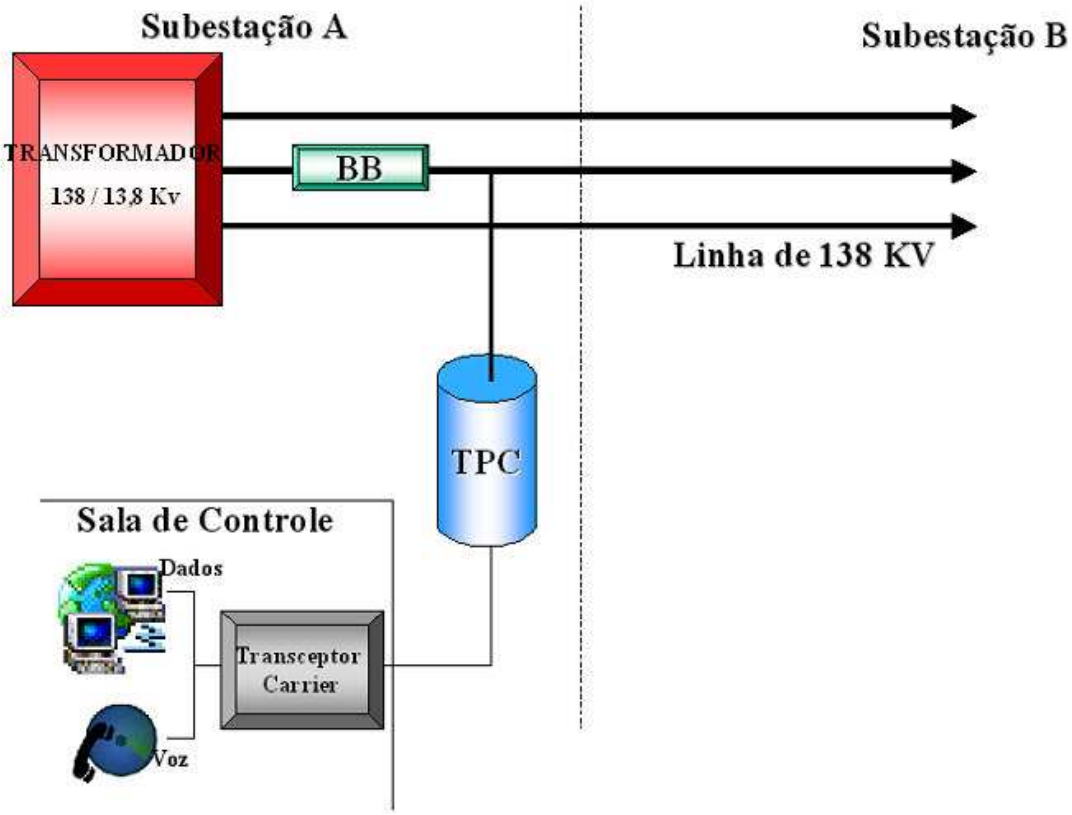


Figura 1: Esquema de funcionamento do Power Line Carrier

Um Transceptor Carrier é instalado depois do TPC. Esse dispositivo tem a função de transformar os sinais provenientes deste TPC, para os meios convencionais de voz e dados, fazendo assim com que seja possível a análise das informações.

Outra forma em que essa tecnologia pode ser usada é através de modems Power Line Carrier. A figura 2 mostra melhor como é feita a ligação com estes tipos de modems.

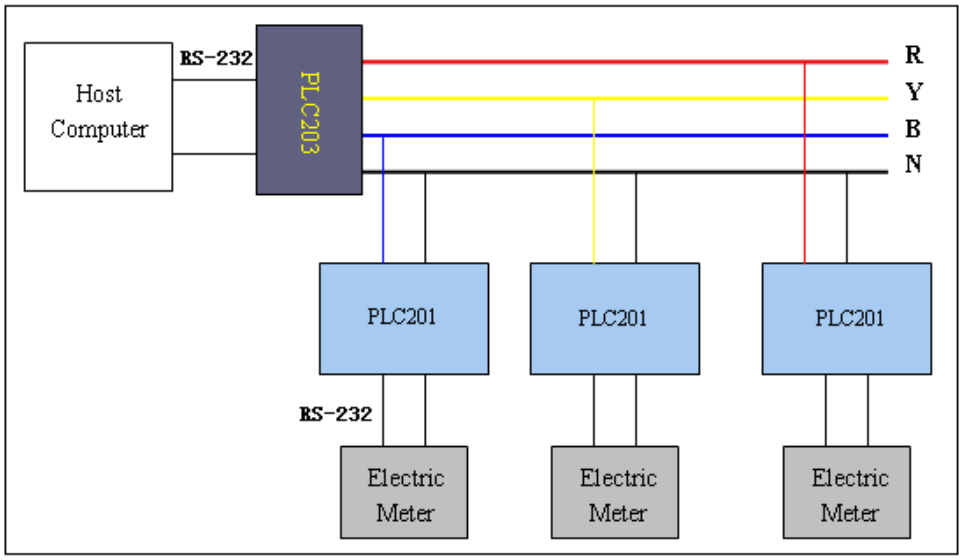


Figura 2: Ligação de esquemas Power Line Carrier através de modems.

Em um sistema trifásico pode-se ligar até 3 aparelhos eletrônicos que se deseja controlar. Liga-se um modem monofásico (PLC201) em cada fase da rede elétrica via interface serial RS-232 a cada aparelho. Na outra ponta liga-se um modem trifásico (PLC203) nas 3 fases da rede elétrica. Nesse modem liga-se o computador que fará o controle / monitoramento desses aparelhos também através de uma interface serial RS-232.

Porém essa tecnologia trabalha com uma taxa muito baixa de transmissão de dados (apenas 9,6 Kbps), o que impossibilita o uso dessa tecnologia para a transmissão de dados em alta velocidade, além de ser pouco utilizada atualmente devido ao barateamento e o avanço da tecnologia de fibras ópticas e dos sistemas de telecomunicações.

Em 1991, baseado no padrão Power Line Carrier, o Dr Paul Brown da Norweb Communications [2] empresa de energia elétrica da cidade de Manchester na Inglaterra, iniciou os testes com a comunicação digital em alta velocidade através da

rede elétrica. Inicialmente ele esbarrou principalmente nos problemas de ruído e interferência.

Entre 1995 e 1997 ficou demonstrada a possibilidade da solução desses problemas e, com isso, tornou-se mais viável a idéia de transmissão de dados em alta velocidade através da rede elétrica.

Em outubro de 1997 a Nortel se juntou a Norweb e anunciaram a resolução dos problemas de ruídos e interferências nas linhas elétricas [2]. Dois meses depois essas empresas em parceria anunciaram o primeiro teste de acesso à internet através da tecnologia de transmissão pela rede elétrica em uma escola de Manchester, assim batizando essa tecnologia de DPL (Digital Power Line). Ainda em 1997 foi criado um fórum na Europa para estimular o desenvolvimento dessa nova tecnologia, chamado PLC Fórum.

Em março de 1998 a Nortel e a Norweb criaram uma nova empresa para desenvolver e comercializar a tecnologia DPL, chamada Nor.Web DPL. Também em 1998 foi criado um fórum chamado Power Line Telecommunications Fórum (PLTF), pela United Telecom Concil (UTC).

Em setembro de 1999 a recém criada APTEL (Associação de Empresas Proprietárias de Infra-Estrutura e de Sistema Privados de Telecomunicações) e o Sub-comitê de Comunicações do GCOI realizaram seu primeiro seminário com um único tema: Power Line Communications Technology.

Em abril de 2003 a Agência Regulatória Federal de Serviços de Telecomunicações (FCC) dos Estados Unidos emitiu diversas declarações favoráveis à tecnologia PLC, e alterou o nome dessa tecnologia para BPL (Broadband over Power Lines).

Atualmente, devido à solidez dessa tecnologia, diversas empresas já comercializam produtos próprios para redes PLC. Também no Brasil existem alguns projetos que já envolve essa tecnologia. Na Europa, mais especificamente na Alemanha, ela até já está comercializada como uma alternativa para acesso de Banda Larga, com taxas de transmissão entre 1Mbps e 3Mbps.

2.2 BASES TECNOLÓGICAS

2.2.1 Modulações

A modulação é a modificação de um sinal eletromagnético de forma que ele possa transportar dados através de um sinal de rádio frequência (onda portadora).

A modulação é responsável por mapear cada possível sequência de bits.

Existem atualmente vários tipos de modulações, mas apenas serão citadas as modulações por chaveamento de frequência (FSK) e por divisão ortogonal de frequência (OFDM).

2.2.1.1 Modulação por Chaveamento de Frequência (FSK)

A modulação FSK atribui frequências diferentes para a portadora em função do bit a ser transmitido. Quando um bit ‘0’ é transmitido a portadora assume uma frequência correspondente a um bit 0 durante o período de duração do bit. Outra frequência é usada na transmissão de um bit ‘1’.

Geralmente são utilizados dois valores de frequência para ‘0’ ou ‘1’. Porém também pode-se utilizar 4 valores de frequências diferentes, cada uma correspondendo a 2 bits (f1 = 00, f2= 01, f3=10, f4=11), o que aumenta a taxa de transmissão de bits mas também aumenta a banda de frequência de transmissão utilizada. Essa modulação é chamada FSK DI-BIT.

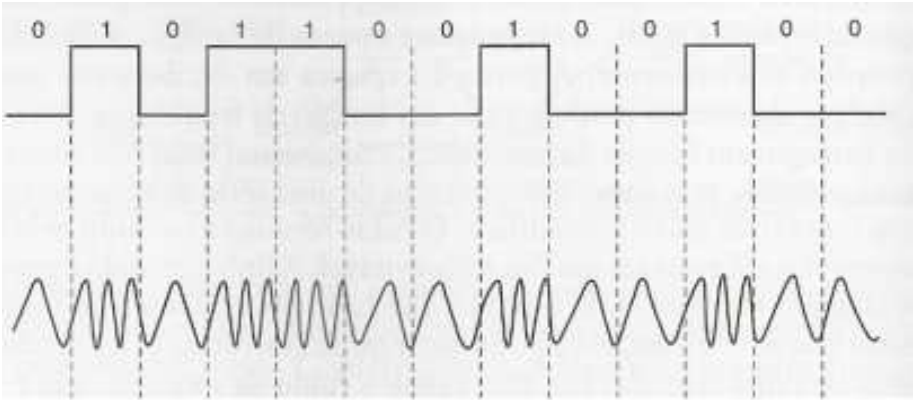


Figura 3: Modulação FSK

2.2.1.2 Modulação por Divisão Ortogonal de Frequência (OFDM)

Consiste em enviar os dados utilizando um conjunto de portadoras de diferentes frequências, onde cada portadora transmite apenas alguns bits do sinal original.

Para evitar interferências as portadoras são ortogonais entre si, isto é, o espaçamento entre as portadoras é igual ao inverso da duração de um símbolo.

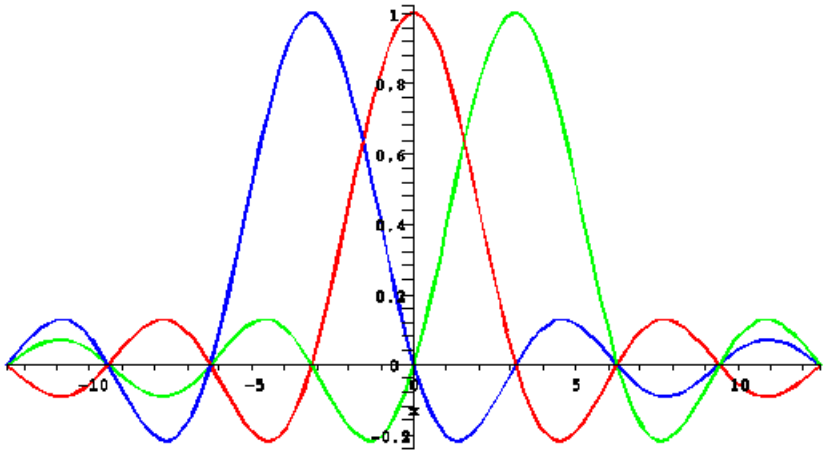


Figura 4: Modulação OFDM

Quando os sinais são modulados nas portadoras, são inseridos pequenos intervalos de tempo entre a informação útil de um bit e a informação útil do bit seguinte. Esse processo reduz a taxa de bits de cada portadora, mas proporciona maior robustez

do sinal com relação a ecos e multipercursos, reduzindo a taxa de erros de transmissão.

2.2.2 Métodos de Transmissão

São os protocolos que são utilizados para se transmitir a informação através de um meio de transmissão qualquer, podendo ser ele por cabo ou pelo ar.

O método de transmissão utilizado pelas redes PLC é o **Acesso Múltiplo à Portadora com Prevenção de Colisão (CSMA/CA).**

Esse tipo de protocolo tem o objetivo de evitar que ocorram colisões no meio de transmissão. Esse mecanismo de acesso possui um esquema de acesso randômico com um sensor do meio que indica se ele está ou não livre naquele momento. A estação quando deseja transmitir ouve o meio de transmissão e aguarda por um instante de tempo chamado DIFS, para ter certeza que o meio de transmissão está livre.

Se o meio estiver ocupado as estações têm que esperar pela duração de DIFS, e depois entrar numa fase de contenção. Cada estação escolhe um tempo aleatório de *backoff*, dentro de uma janela de contenção, e tenta acessar o meio depois de passado esse intervalo de tempo escolhido. Se passado esse intervalo de tempo o meio ainda estiver ocupado, essa estação perdeu esse ciclo e terá de esperar por pelo menos um período DIFS. Caso o meio esteja inativo depois de passado esse intervalo de tempo, essa estação pode acessar o meio imediatamente e assim começar a transmissão.

Esse tempo de espera aleatório é escolhido como sendo um múltiplo de um *slot time*, que é o derivado do atraso de propagação do meio, atraso de transmissão e outros parâmetros dependentes do meio físico.

A figura 5 representa o mecanismo básico do CSMA-CA.

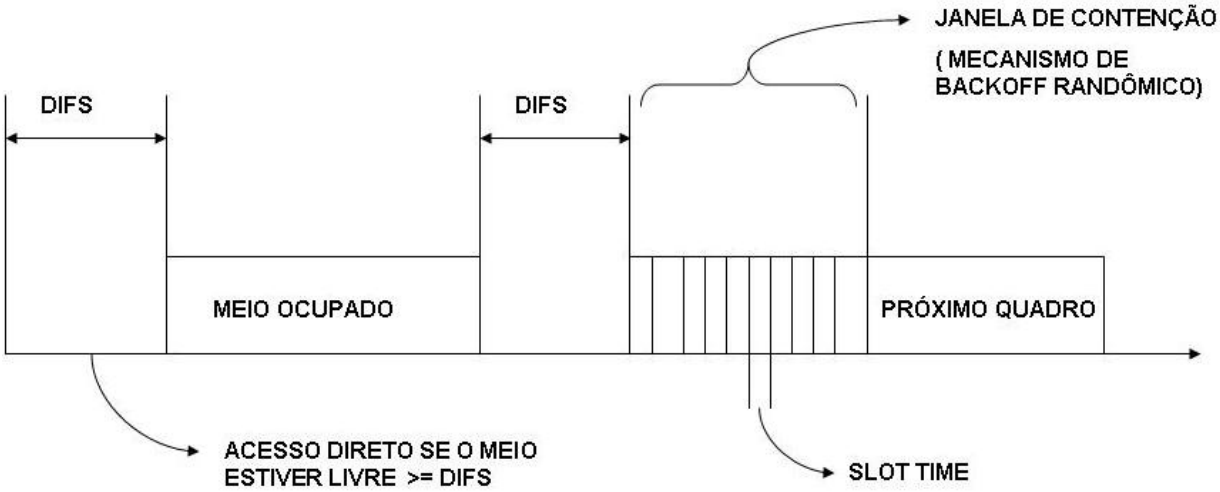


Figura 5: Esquema de transmissão CSMA-CA

Dessa forma as outras estações não tentarão transmitir pois sabem que o meio está sendo utilizado por outra estação, porém o tempo que uma máquina espera para poder transmitir é conhecido, fazendo com que ela não espere pelo meio quando o mesmo está livre.

2.2.3 Métodos de Criptografia

São métodos de transformar a informação para uma forma aparentemente ilegível, podendo ser lida apenas pelo destinatário da informação.

O objetivo desses métodos é preservar a confidencialidade da informação, pois mesmo que haja interceptação do pacote por um usuário não autorizado, o mesmo não irá conseguir processar essa informação, uma vez que ele não saberá qual é o método de descriptografia que tem que ser utilizado para tornar legível aquele pacote.

2.2.3.1 Padrão de Criptografia de Dados (DES)

É baseado em uma cifra de 128 bits desenvolvida e patenteada pela IBM, cujo nome é Lúcifer. Foi adotado pelo governo dos Estados Unidos em janeiro de 1977 depois de uma redução da chave para 56 bits.

É um algoritmo de chave simétrica, isto é, utilizada uma mesma chave de criptografia para codificar e decodificar os dados. Trabalha através da troca de chaves onde o usuário que deseja enviar os dados possui uma chave para criptografar, e o usuário que irá receber esses dados deverá conhecer essa chave para descriptografá-los.

O DES trabalha com uma chave de 64 bits, porém o tamanho efetivo dessa chave é de 56 bits, pois os outros 8 bits restantes são utilizados para verificação de paridade e descartados em seguida.

O algoritmo criptografa o texto simples em blocos de 64 bits, produzindo 64 bits de texto cifrado. O algoritmo, parametrizado por uma chave de 56 bits, tem 19 fases distintas. A primeira fase é uma transposição independente da chave de texto simples de 64 bits. A última fase é exatamente o oposto dessa transposição. Na penúltima fase se troca os 32 bits mais à esquerda pelos 32 bits mais à direita. As outras 16 fases são funcionalmente iguais, mas são parametrizadas por diferentes funções da chave.

A figura 6 ilustra o funcionamento de um algoritmo de Criptografia DES.

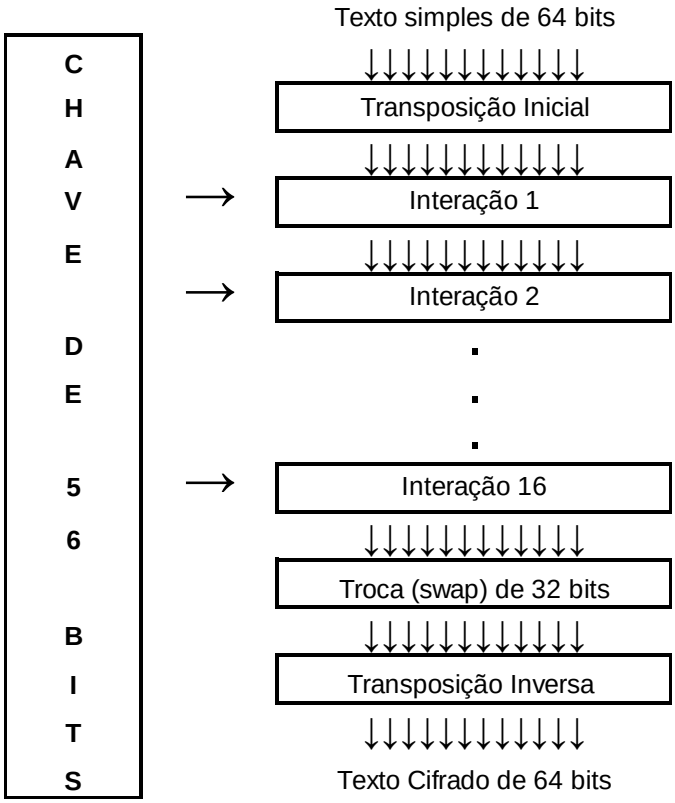


Figura 6: Algoritmo de Criptografia DES

Para descriptografar os dados o algoritmo simplesmente executa as etapas na ordem inversa.

2.2.3.2 Padrão de Criptografia Avançada (AES)

Em janeiro de 1997 pesquisadores do mundo inteiro foram convidados e patrocinados pela NIST (National Institute os Standards na Technology) a submeter propostas para um novo padrão de criptografia, a ser chamado AES [14].

Foi desenvolvido um concurso onde as regras eram:

- O algoritmo teria de ser uma cifra de bloco simétrica.
- Todo o projeto deveria de ser público.
- Deveriam ser admitidos tamanhos de chaves de 128, 192 e 256 bits.

- Teriam de ser possíveis implementações de software e de hardware.
- O algoritmo teria de ser público ou licenciado em termos não discriminatórios.

Ao final desse concurso o algoritmo de Rijndael foi o mais votado, inclusive recebendo voto da NIST. Em novembro de 2001 esse algoritmo se tornou um padrão do Governo dos Estados Unidos.

Rijndael admite tamanhos de chaves e tamanhos de blocos desde 128 bits até 256 bits em intervalos de 32 bits. O comprimento da chave e do bloco pode ser escolhido independentemente.

O AES especifica que o tamanho do bloco deve ser de 128 bits e o comprimento da chave deve ser 128, 192 ou 256 bits. É pouco provável que alguém utilize chaves de 192 bits. Assim o AES tem duas variantes: um bloco de 128 bits com uma chave de 128 bits e um bloco de 128 bits com uma chave de 256 bits.

Como o DES, o Rijndael utiliza substituição e permutações, e também emprega várias rodadas. O número de rodadas depende do tamanho da chave e do tamanho do bloco, sendo 10 para chaves e blocos de 128 bits, passando para 14 no caso da maior chave ou do maior bloco. Todas as operações envolvem bytes inteiros a fim de permitir implementações eficientes tanto em hardware quanto em software.

Esse algoritmo foi projetado não só por segurança mas também para aumentar a velocidade, podendo em uma implementação via software em uma máquina de 2GHz alcançar uma taxa de criptografia de 700 Mbps, e ainda mais rápida nas implementações via hardware.

2.3 APLICAÇÕES E SERVIÇOS OFERECIDOS

2.3.1 Aplicações Residenciais e SOHO

Assim como as redes cabeadas, a principal aplicação das redes Powerline é funcionar como uma Lan operando em altas taxas de transferência.

Podemos utilizar as redes Powerline da mesma forma que é usada a rede cabeada e wireless, utilizando os serviços existentes que necessitam de uma rede confiável, com baixas taxas de erros e alta velocidade de transmissão, entre eles, VoIP, monitoramento com câmeras de segurança IP, TV digital, banda larga, rede local, e a idéia futura de conectar eletrodomésticos na rede para obter informações desses aparelhos e programá-los remotamente.

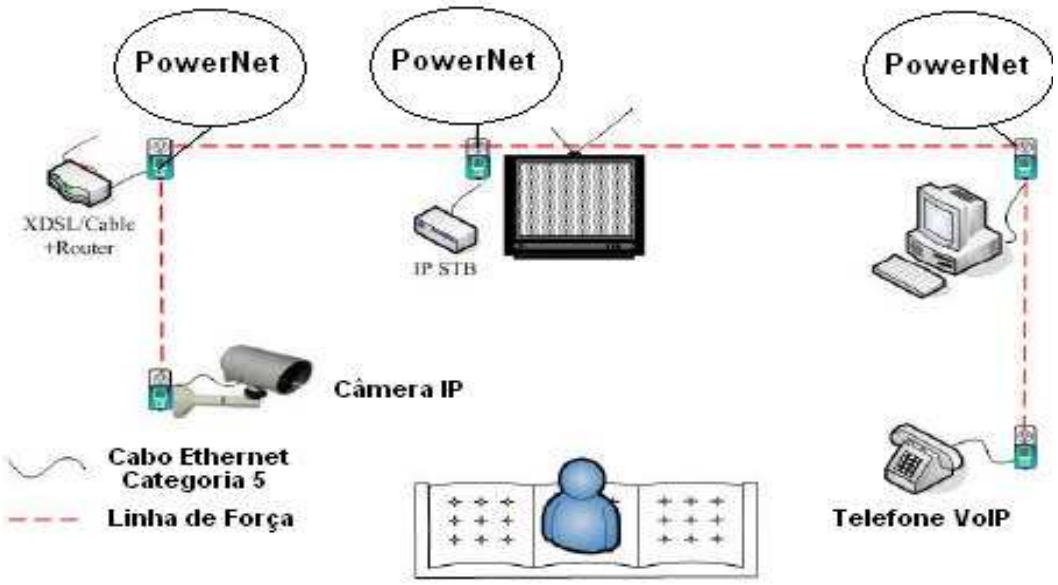


Figura 7: Exemplo de uma rede PLC em soluções residenciais.

Conforme podemos ver como exemplo no esquema da figura 7, todos os aparelhos estão ligados em um mesmo circuito de energia. Essas aplicações podem ser utilizadas tanto para uso residencial, quanto para uso coorporativo.

2.3.2 Serviços Oferecidos

Outro setor que deverá lucrar e se desenvolver muito com a chegada dessa nova tecnologia serão as concessionárias de energia elétrica, pois aumentará a gama de serviços que elas poderão oferecer ao usuário final, como por exemplo, serviços de conexão à internet banda larga, serviços de telefonia usando principalmente VoIP, serviços de gerenciamento de energia, entre outros.

Podemos ver na figura 8 como ficaria o esquema da rede de distribuição de uma concessionária de energia desde a subestação.

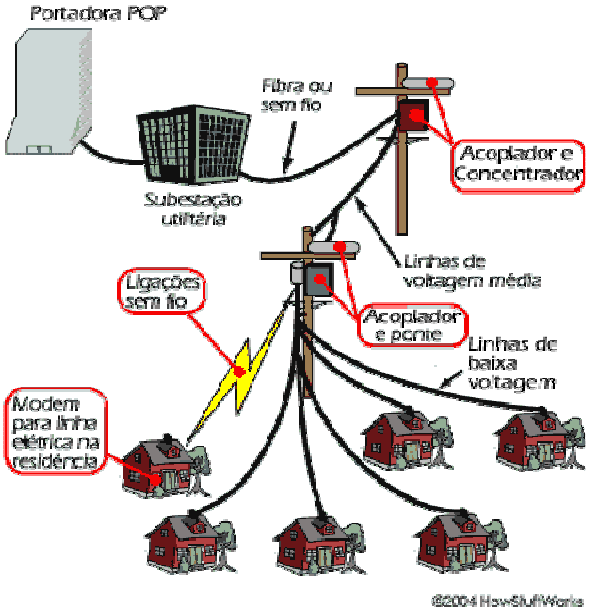


Figura 8: Exemplo de uma rede de serviços de uma concessionária

Outra função que a tecnologia PLC pode oferecer é a capacidade de leitura dinâmica dos medidores de energia. Com essa leitura as empresas fornecedoras de energia elétrica conseguirão aumentar substancialmente a melhoria da eficiência energética, e com isso melhorar a recuperação de perdas de energia, tanto em cabos e equipamentos que não estejam funcionando perfeitamente, quanto ajudando a combater os famosos “gatos”.

3 TECNOLOGIAS PLC INDOOR

Surgiram como uma alternativa as redes cabeadas e wireless, sendo um novo tipo de infra-estrutura de cabeamento para rede Local LAN.

Atualmente conseguimos trafegar dados em uma rede local com taxas de até 200 Mbps, utilizando como meio físico os cabos elétricos que utilizamos nas instalações elétricas. Fora essa boa taxa de transmissão tem-se também um ótimo alcance, pois se consegue cobrir distâncias de até 300 metros.

As redes PLC trabalham na camada de enlace do modelo OSI (Interconexão de Sistemas Abertos), sendo assim elas podem perfeitamente ser agregadas a uma rede TCP/IP já existente. Elas são compatíveis com as outras tecnologias que trabalham na camada de enlace, por isso consegue-se misturar outros meios físicos como, por exemplo, meios cabeados (UTP, Coaxiais, Ópticos) e wireless, com a rede PLC.

Porém existem alguns problemas como ruídos e interferências no uso desta tecnologia, pois os cabos elétricos geralmente são feitos com uma variedade de tipos de condutores e normalmente esses condutores não têm as mesmas características técnicas, pois um meio pode apresentar maior interferência em um ponto em relação ao outro.

As características do canal de transmissão podem variar de acordo com o tempo em que as cargas elétricas sofrem alterações na rede elétrica. Além disso, os sinais transmitidos podem sofrer interferência de alguns equipamentos elétricos como motores, lâmpadas de halogênio e rádio amadores, por exemplo.

Também precisamos ter cuidado quanto às emendas na rede elétrica e ao uso de extensões e benjamins, pois eles criam pontos de reflexão causando ecos do sinal e posteriormente a perda de pacotes.

No-breaks, estabilizadores e filtros de linha bloqueiam os sinais de alta frequência, e por isso não se pode ligar equipamentos PLC nesses equipamentos.

3.1 TECNOLOGIA PASSPORT

Tecnologia desenvolvida pela empresa Intelogis [4], funciona através da modulação FSK utilizando duas frequências, uma para 1s e outra para 0s. As frequências utilizadas pelas redes Passport estão em uma largura de banda estreita logo acima do nível onde ocorre a maior parte dos ruídos de linha. Este método é considerado frágil, pois qualquer coisa que possa afetar a frequência pode interromper o fluxo de dados, fazendo com que haja uma retransmissão. Por exemplo, quando se liga um aparelho que consome uma maior potência, como um chuveiro elétrico ou uma lavadora de roupas, a rede perde pacotes devido à interferência que esses aparelhos causam.

Como uma solução para isso, a Intelogis incluiu extensões elétricas com condicionamento de sinal em seu kit de rede, e aconselha inseri-las entre a tomada elétrica e o computador para ajudar a reduzir os ruídos provenientes da rede elétrica.

Figura 9: Dispositivo Passport (SmartComputing)

O tipo de ligação é feita através de um cabo paralelo que é ligado a um dispositivo conectado na tomada elétrica e a outra ponta é ligada à porta paralela do computador, conforme mostra a figura 9.

Também podemos ligar uma impressora paralela a um dispositivo Passport, porém ela não irá trabalhar com impressões bidirecionais. Com isso a impressora não enviará ao computador informações como quantidade de tinta restante ou falta de papel.

Vale lembrar também que o dispositivo Passport tem que ser ligado diretamente na porta paralela do computador.

A tecnologia passport trabalha com uma arquitetura de cliente-servidor. A primeira máquina onde é instalado o software se torna o Servidor de Aplicação que controla o fluxo de dados e contata cada dispositivo de rede onde pode achar os outros dispositivos.

Entretanto, alguns problemas com essa tecnologia fizeram com que ela não fosse o padrão para redes PLC, como por exemplo:

- Velocidade de conexão relativamente baixa: entre 50Kbps e 350Kbps.
- Performance impactada pelo uso de dispositivos na rede elétrica.
- Só trabalha com computadores com o sistema operacional Windows.
- Só pode ser usada em redes 110V.
- Requer que todos os dados sejam encriptados para uma rede segura.

3.2 TECNOLOGIA POWERPACKET

Foi desenvolvida pela Intellon [4] que recentemente foi adquirida pela empresa norte americana Atheros. Usa uma forma aumentada de multiplexação de divisão de

frequêncial orthogonal (OFDM), com um esquema de correção de erros semelhante ao encontrado na tecnologia DSL.

O OFDM trabalha nas faixas de frequência de 4.3MHz à 20.9MHz. Ele envia uma série de pacotes de dados simultaneamente com várias frequências transportadas. Quando ocorre um rompimento em uma das frequências utilizadas por causa de um ruído ou uma oscilação de energia que ocasiona a perda de um pedaço do pacote, o PowerPacket sente falta de pedaço do pacote e troca dados para a retransmissão desse pedaço perdido. Com isso é permitida uma maior velocidade e confiabilidade na entrega do pacote.

Os dispositivos PowerPacket trabalham com uma taxa de transmissão de 14Mbps, e sua conexão física com um computador é feita através de uma porta Ethernet ou USB, ou através da instalação de uma placa PCI PowerPacket no computador do usuário, conforme na figura 10.

Figura 10: Dispositivo PowerPacket

Depois da instalação física do equipamento, a instalação do software é bem simples, e ele automaticamente encontra os computadores e impressoras na rede.

Esta tecnologia funciona como uma arquitetura de rede semelhante às redes ponto-a-ponto.

As maiores vantagens dessa tecnologia em relação à tecnologia Passport são:

- Compatível com outros sistemas operacionais (dependendo do driver).
- Inclui encriptação dos dados.
- Trabalha independente da voltagem de linha e da frequência de corrente.
- Pode-se usar a impressora com todos os seus recursos.
- Maior velocidade de transmissão de dados (14Mbps contra 350Kbps).
- Não se tem perdas na velocidade de transmissão com a ligação de outros aparelhos.

3.3 TECNOLOGIA HD-PLC (HIGH DEFINITION POWER LINE COMMUNICATION)

Criada em julho de 2005 esta tecnologia é uma solução em redes PLC criada pela Panasonic [9]. Atualmente ela é a maior concorrente do padrão Homeplug. Assim como o Homeplug ela trabalha nas portas ethernet ou USB, conseguindo atingir taxas teóricas de até 210Mbps, cobrindo distâncias de aproximadamente 150 metros.

Esta tecnologia adota como meio de modulação o “Wavelet OFDM” utilizando faixas de frequências de 4 MHz a 28 MHz.

Um filtro de corte programável previne as interferências desta tecnologia com outras transmissões de rádio frequência como o rádio amador.

Para tratar dos ruídos no meio de comunicação, foi criada uma tecnologia de estimativa do canal que estima os ruídos de transmissão nas linhas elétricas. O método de estimação aprende as características da linha e calcula, em função da relação de pacotes enviados e recebidos, uma quantidade máxima de dados para atingir cada sub-portadora, com isso ela consegue maximizar a taxa de transmissão desses dados.

Quanto ao método de acesso, ela trabalha com uma arquitetura híbrida, combinando o TDMA (Acesso Múltiplo por Divisão de Tempo), com o CSMA / CA (Acesso Múltiplo à Portadora com Prevenção de Colisão), para garantir melhor QoS (qualidade de serviço).

Para garantir a segurança e a confidencialidade da comunicação, a tecnologia de transmissão HD-PLC utiliza um algoritmo de criptografia AES com 128bits. A figura 11 mostra um equipamento HD-PLC

Figura 11: Equipamento HD_PLC (Panasonic-2007)

3.4 TECNOLOGIA HOMEPLUG

No primeiro trimestre de 2001 uma associação de grandes empresas em TI, como a Cisco System, Intel, Samsung, Huawei, Motorola, entres outras, se uniram e criaram a Homeplug Powerline Alliance [13], com o objetivo de criar um padrão de indústria para a fabricação de equipamentos para redes de dados através da infra-estrutura da rede elétrica. Essa aliança criou o padrão Homeplug v1. 0.

Por ser a tecnologia PLC mais usada atualmente a tecnologia Homeplug será vista com mais detalhes no capítulo 4.

4 TECNOLOGIA HOMEPLUG

4.1 CAMADA FÍSICA

O OFDM é a técnica de transmissão usada no padrão Homeplug, utilizando 84 sub-portadoras igualmente espaçadas com frequências de banda entre 4.5 MHz e 21 MHz.

Prefixos cíclicos e técnicas de modulação diferenciais, como DBPSK e o DQPSK, são utilizados para eliminar completamente a necessidade de qualquer equalização. Ruídos são evitados através de técnicas de correção antecipada de erros FEC (Forward Error Correction) e técnicas de intercalação de dados.

A tecnologia Homeplug otimiza a velocidade de transmissão dos dados em cada link através de uma abordagem adaptativa obtida através da modulação, da técnica de correção antecipada de erros (FEC), e de uma atribuição TONE, que é um processo onde algumas das portadoras danificadas são desligadas.

Essa atribuição TONE faz com que se tenha uma redução da taxa de erros dos bits enviados, ajudando na FEC e nas opções de modulação das portadoras boas.

O protocolo de controle de acesso ao meio (MAC) do Homeplug é modelado para trabalhar com formatos de frame no padrão IEEE 802.3. O protocolo MAC do Homeplug criptografa e acrescenta bits de gerenciamento aos quadros ethernet antes de transmiti-lo através da rede elétrica. Além disso, a segmentação de pacotes e a remontagem dos mesmos são utilizadas quando um pacote completo não cabe em um único quadro.

4.2 FORMATOS DOS QUADROS

São utilizados 2 formatos de quadros. O formato longo de quadro é constituído pelo delimitador de início do quadro (SOF), a carga útil (Payload), e o delimitador de fim do quadro (EOF). Já o formato curto de quadro é constituído de um delimitador de resposta e é usado como parte do processo ARQ, que é o processo de retransmissão dos pacotes corrompidos.

Um delimitador é formado pelo preâmbulo e pelo campo de informação de controle de frame. A função do preâmbulo é indicar o início de um delimitador, logo após o preâmbulo vêm às informações de controle do quadro. Essas informações são codificadas e podem ser detectadas mesmo com um alto ruído na linha de transmissão.

A função dos delimitadores é indicar a prioridade do tráfego no meio e o tempo necessário para efetuar aquela transmissão. A informação passada pelos delimitadores é utilizada pelo protocolo MAC para determinar a disponibilidade do meio, reduzindo assim à quantidade de colisões.

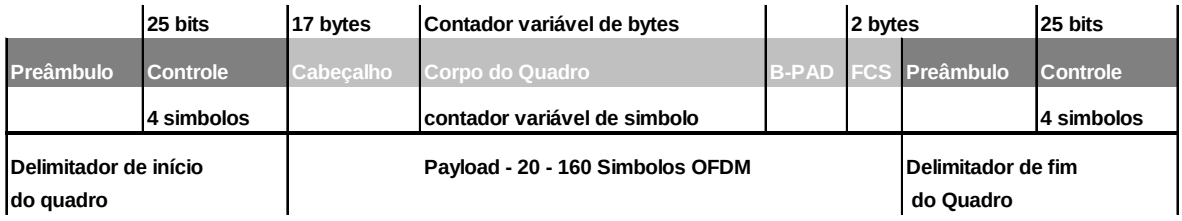


Figura 12: Exemplo de formato longo de quadro

Conforme podemos ver na figura 12, os primeiros 17 bytes da carga útil (payload) são designados para o cabeçalho do quadro que carrega informações como endereço de origem, endereço de destino e segmentação do pacote.

Para garantir uma melhor garantia de QoS (qualidade de serviço), a tecnologia Homeplug limita o campo de Payload em 160 símbolos OFDM. Quando se deseja enviar um pacote maior que esses 160 símbolos é utilizada a técnica de segmentação e remontagem dos pacotes. Além disso, os dados são protegidos por uma sequência de verificação dos quadros (FCS), que detecta erros incorrigíveis no quadro.

4.3 MECANISMO DE ACESSO

Para controlar o acesso ao meio a tecnologia Homeplug utiliza uma variante do protocolo CSMA / CA, que é formado por um mecanismo de detecção, um mecanismo de prioridade e um algoritmo de backoff.

A tecnologia Homeplug utiliza uma combinação com o sentido físico da portadora PCS (Physical Carrier Sense) e o sentido virtual da portadora VCS (Virtual Carrier Sense), determinando assim se o meio está ou não ocupado e em quanto tempo ele ficará livre.

O PCS é informado através da camada física do Homeplug. Ele indica se um sinal preâmbulo é detectado no meio. O VCS é informado pela camada MAC e é atualizado através das informações contidas no delimitador do quadro.

O mecanismo de prioridade prioriza o acesso ao meio de uma forma altamente distribuída, sem a necessidade de um nó central para coordenar o acesso ao meio, como acontece em algumas tecnologias de rede.

Tabela 1: Informações sobre controle de quadros

Tipo de Delimitador	Campos	Siginificado
Início do Quadro (SOF)	Tipo	Um indicador de um quadro curto indica se o SEOF é com ou sem resposta esperada.Ele é esperado ao final de um quadro longo.
	Controle de Contenção	Quando é setado (1), dá prioridade na transmissão ao nó que está transmitindo impedindo que nós com prioridade menor ganhem acesso ao meio entre uma transmissão e outra.
	Tamanho de quadro	Indica o tamanho do payload em múltiplos blocos de símbolo OFDM.
	Mapeamento do Índice TONE	Contém as informações de adaptação dos canais. O payload é codificado utilizando as taxas máximas de transfe-rência que podem ser feitas no link.
Final do Quadro (EOF)	Tipo	Como o SOF, é um indicador de um quadro curto e indica se o EOF é com ou sem resposta esperada. Também é esperado ao final de um quadro longo.
	Controle de Contenção	Envia o mesmo tipo de informação que um delimitador SOF, ajudando na melhor sincronização.
	Prioridade de Acesso ao canal (CAP)	Indica a prioridade no quadro longo atual.
Resposta (RESP)	Tipo	Pode ser do Tipo ACK (pacote enviado), do tipo NACK (falha na recepção do pacote), ou do tipo FAIL (falha na recepção por falta de recursos)
	Prioridade de Acesso ao canal (CAP)	Indica a prioridade do quadro longo anterior.

O padrão Homeplug permite até quatro diferentes níveis de prioridade. Os slots de resolução prioritária (PRS) e os sinais de resolução prioritária são o coração desse mecanismo de resolução de prioridades.

Os sinais de resolução prioritária usam uma forma de sinal *spread spectrum* que têm alta tolerância ao atraso de transmissão, e impedem a propagação da interferência destrutiva que ocorre quando vários nós desejam transmitir ao mesmo tempo. Após o final de cada transmissão dois slots são alocados para resolução de prioridade.

Após esses slots de resolução prioritária, a disputa pelo acesso ao meio será apenas entre os nós que têm uma maior prioridade na rede. Por exemplo, quando as 4 prioridades estão presentes na rede, os nós com prioridade 2 e 3 enviam sinais de resolução prioritária em PRS0 (slot de resolução prioritária 0). Os nós com prioridade 0 e 1 irão detectar esses sinais e atrasarão suas transmissões para que os nós com maior prioridade transmitam. Os nós com prioridade 3 transmitirão sinais de resolução prioritária em PRS1(slot de resolução prioritária 1), que será detectado pelos nós de prioridade 2, fazendo com que ele adie sua transmissão. Assim apenas os nós com prioridade 3 irão concorrer ao acesso ao meio, no período de contenção.

O padrão MAC Homeplug fornece informações sobre prioridade de quadros utilizando Tags de Vlan´s, conforme definido no padrão 802.1Q, através das camadas de rede mais altas.

Tabela 2: Recomendações sobre prioridade para o Homeplug

Prioridade de acesso ao canal Powerline	Prioridades Manuais (por tags de Vlan)	Classes de Aplicações
Prioridade 3	7,6	Voz: caracterizada por um atraso e jitter menor que 10msec (ex: VoIP)
Prioridade 2	4,5	Audio e Vídeo: caracterizado por um atraso menor que 100msec
Prioridade 1	0,3	Transferências em massa
Prioridade 0	1,2	Tráfego de melhor esforço

Foi implementado um algoritmo de backoff que se adapta aos níveis de prioridade dos aplicativos para garantir uma maior utilização, e evitar o congestionamento da rede.

Assim como nos outros algoritmos CSMA / CA, o slot backoff é um número randômico inteiro que varia de 0 até o tamanho da janela de contenção. O crescimento dessa janela é controlado pela estimativa do tráfego na rede. Esse algoritmo ajuda a alcançar melhor utilização da rede e a controlar a latência para o tráfego de maior prioridade.

4.4 MECANISMOS DE SEGMENTAÇÃO E REMONTAGEM DOS PACOTES

Muitas das vezes são enviados pacotes maiores do que o tamanho máximo que cada quadro pode transportar. Quando isso ocorre, é necessário segmentarmos os pacotes e enviá-los em mais de um quadro, ficando o receptor com trabalho de remontagem desses pacotes.

Para fazer a remontagem do pacote o receptor utiliza as informações que ele obtém no campo de controle que fica no cabeçalho do quadro.

Para aumentar a taxa de transferência (throughput) da rede, vários segmentos podem ser enviados em uma única rajada, porém cada segmento tem que passar pelo mecanismo de resolução prioritária para garantir que a rajada seja interrompida quando for necessário transmitir um tráfego de maior prioridade.

4.5 RECURSOS DE QoS

Uma das preocupações na elaboração da tecnologia Homeplug era garantir bons níveis de QoS, para que a tecnologia pudesse suportar aplicações que necessitam de tráfego prioritário, como o VOIP por exemplo. Podemos ver abaixo as principais características de QoS que a tecnologia suporta:

- Suporta até 4 níveis de prioridade baseadas em tags Vlan.
- Acesso completamente distribuído reduzindo a complexidade de implementação.
- Suporte opcional para contenção de livre acesso.
- Algoritmo agressivo de backoff que garante latências mais baixas para o tráfego de maior prioridade.
- Segmentação e remontagem dos pacotes.
- Descarta pacotes de tempos diferentes e trabalha com um limite máximo de repetição que garante que pacotes excessivamente atrasados sejam descartados.

4.6 PERFORMANCE

A HomePlug Powerline Alliance [13] executou diversas medidas de desempenho de throughput para verificar a performance da tecnologia. As medições de desempenho de throughput realizadas foram as seguintes:

- Throughput da Camada Física → É a taxa de transferência de um dado no payload de um quadro longo.

Tabela 3: Throughput da Camada Física com vários tipos de Modulação e FEC

	Modulação	FEC	Mbps
DQPSK 3/4	DQPSK	3/4 Código Convolucional e Código de Reed Salomon	13.78
DQPSK 1/2	DQPSK	1/2 Código Convolucional e Código de Reed Salomon	9.19
DBPSK 1/2	DBPSK	Código Convolucional e Código de Reed Salomon	4.59
ROBO	DBPSK	1/2 Código Convolucional, Código de Reed Salomon e cada bit é repetido 4 vezes	1.02

- Throughput da Camada MAC → É a taxa onde os quadros Ethernet são transmitidos.
- Throughput da Camada TCP → É a taxa onde o payload TCP é transferido.

Tabela 4: Throuput de Diferentes Camadas

	Throughput (Mbps)
Throughput da Camada Física	13.78
Throughput da Camada MAC	8.2
Throughput da Camada TCP	6.2

Tabela 5: Comparação de Throughput entre o Homeplug e outras tecnologias

	Homeplug	10 Mbps Ethernet	IEEE 802.1b	HomePNA (4 baud)
Camada Física	13.78	10	11	32
Camada MAC	8.2	9.8	7.48	26.9

4.7 SEGURANÇA

Como o meio físico utilizado pelo padrão Homeplug é compartilhado, a privacidade e a segurança das redes Homeplug são garantidas através da criação de redes lógicas com uma criptografia de dados padrão de 56 bits (56-bit DES) dentro da mesma rede física.

Cada estação mantém uma tabela de chaves de criptografia relacionadas a valores de Seleção de Chaves de Criptografia (EKS). Os valores EKS são usados como índice ou identificador de cada chave de criptografia. Quando um quadro é transmitido uma chave de criptografia é usada para criptografar o conteúdo da mensagem e sua EKS associada é incluída no cabeçalho do quadro. O receptor da mensagem utiliza o EKS para selecionar a chave de criptografia associada da tabela de chaves de criptografia para decriptografar o conteúdo daquela mensagem.

Tabela 6: Exemplo de uma tabela de chaves de criptografia

EKS	Chave de Criptografia	Comentários
0x00	0x08856DAF7CF58185	Chave de Criptografia Default (uma para cada dispositivo)
0x01	0x46D613E0F84A764C	Chave de Criptografia da Rede (uma para toda rede lógica)
…	…	…
0xFF	…	…

Todas as transmissões de uma rede lógica Homeplug são criptografadas através de uma Chave de Criptografia de Rede (NEK). Uma única NEK é utilizada em toda uma rede lógica. Para participar de uma rede lógica, uma estação precisa ter uma NEK e um EKS associados para essa rede.

O Homeplug utiliza senhas ASCII para gerar chaves de criptografia. As chaves são geradas através de senhas utilizadas pelo padrão industrial de criptografia e algoritmos de hash. Assim os usuários conseguem gravar suas senhas da rede lógica de uma forma mais fácil.

A maior parte dos dispositivos Homeplug vem com uma senha de rede comum para gerar um NEK usando EKS 0x01. Isso faz com que se tenha uma comunicação instantânea entre os dispositivos, porém o uso dessa senha não garante a privacidade da sua rede lógica por se tratar de uma senha comum a todos os dispositivos Homeplug. É aconselhável alterar essa configuração criando uma senha única para toda a rede lógica. Esta senha tem que ser configurada em cada estação.

A informação de troca de chaves é passada pela rede física através de quadros de gerência que utilizam chaves privadas de criptografia conhecidas como Padrão de Criptografia de Chaves (DEK), que é programada de fábrica para ser única em cada dispositivo Homeplug.

O dispositivo responsável pelo envio dos quadros de gestão reconhece o DEK de cada estação, e a estação receptora decodifica o quadro recebido com seu DEK. O DEK é utilizado apenas para troca segura de chaves NEK na rede elétrica.

Outro nível de segurança vem da exclusividade do canal entre quaisquer 2 estações na rede. O processo de estimativa do canal entre 2 estações resulta em um par de mapas TONE para portadoras usáveis, taxas de codificação FEC, e métodos de modulação, que são usados pelas estações para cada direção da comunicação. Mapas TONE são sempre reavaliados nas mudanças naturais das linhas elétricas. Como resultado, se uma terceira estação tentar controlar ou entrar nessa comunicação a partir de outro ponto na rede, será exigido seu próprio Mapa Tone que vai ser diferente do Mapa Tone anterior.

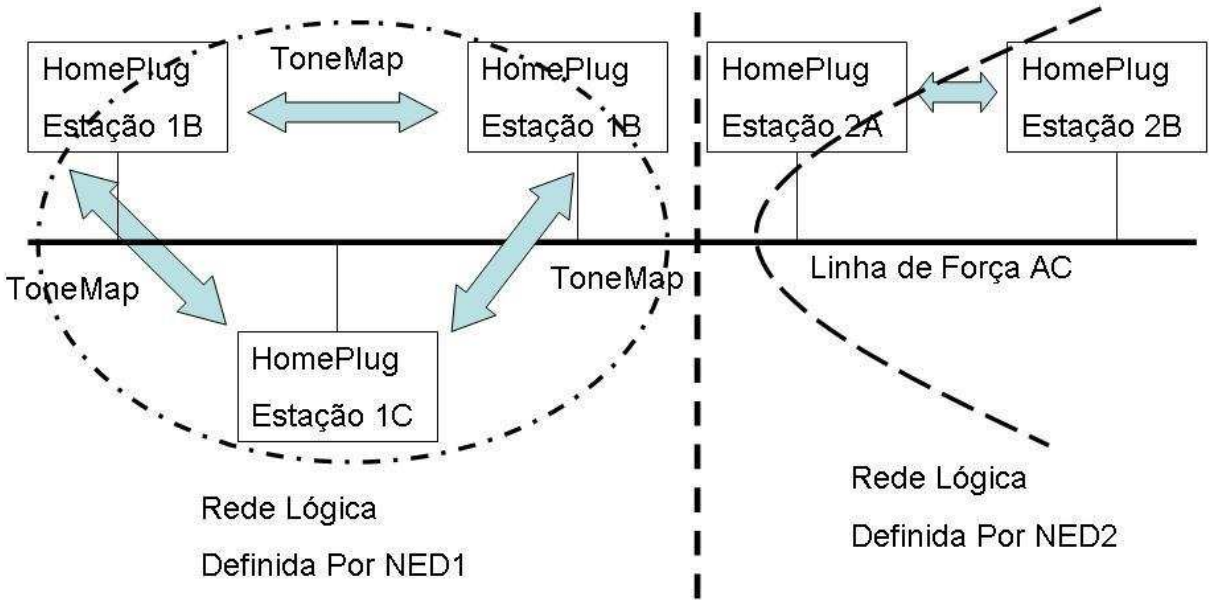


Figura 13: Redes Lógicas Homeplug

4.8 TESTES DE CAMPO

Voluntários e coordenadores do Homeplug realizaram testes de conexão em aproximadamente 7000 caminhos diferentes de comunicação por meios elétricos, em 500 casas ao longo dos EUA e Canadá [13].

Esses testes foram realizados com um par de dispositivos Homeplug, e teve como objetivo verificar o rendimento da conexão por meios elétricos. Foi constatado que a taxa máxima de transmissão que a tecnologia Homeplug suporta é cerca de 8,2Mbps.

Dos 6990 caminhos testados, cerca de 1000 caminhos conseguiram alcançar essa taxa máxima de transmissão.

Além da quantidade de caminhos que conseguiram alcançar a taxa máxima de transmissão, esses testes mostraram que:

- 77% dos links de linhas de energia podem suportar pelo menos 5Mbps de throughput MAC.
- 98% dos links de linhas de energia podem suportar pelo menos 1.5Mbps de throughput MAC.

5 PLC OUTDOOR (BPL)

Quando expandimos os horizontes das redes PLC além uma rede local, onde utilizamos os meios elétricos públicos para trafegar as informações, dizemos que estamos em uma conexão BPL (Banda Larga através de Linhas de Energia).

Essas conexões BPL seguem os mesmos padrões de segurança, formato de quadros, modulação, etc., que utiliza a tecnologia Homeplug.

Companhias de Rede Elétrica, em conjunto com as Companhias de Telecomunicações, podem utilizar o meio elétrico para agregar novos serviços através da rede elétrica, como por exemplo, serviços de telefonia (VoIP), acesso banda larga, tv digital, entre outros.

Esse tipo de conexão também pode ser utilizado pelas Companhias de Rede Elétrica para prover uma melhor distribuição de energia e um melhor atendimento ao seu cliente por meio dos grids inteligentes, assunto que veremos mais à frente.

5.1 FUNCIONAMENTO DE UMA REDE BPL

Para se ter uma conexão de dados e voz através da rede elétrica, a Prestadora de Serviços de Telecomunicações injeta sinais BPL na fiação elétrica através dos injetores BPL, que são aparelhos que adaptam o sinal de internet à frequência necessária para envio através das linhas elétricas e injeta esses sinais no meio elétrico.

Durante toda a extensão da fiação elétrica temos os repetidores BPL que são responsáveis em amplificar o sinal BPL e não deixar que os transformadores filtrem os sinais de alta frequência, pois são esses sinais que são utilizados para a transmissão. Chegando perto do cliente final um master BPL extrai o sinal da rede elétrica pública, identifica os modems que estão sendo utilizados e distribui o sinal BPL para esses modems.

Após ser extraído, o sinal caminha por um cabo de fibra óptica, ou por wireless, ou pela própria fiação elétrica até o modem BPL que fica localizado no cliente final. Esse modem é que faz a conversão do sinal para que o mesmo possa ser usado pelo computador e assim conectando o cliente à internet via banda larga.

Podemos ver melhor esse funcionamento através da figura 14.

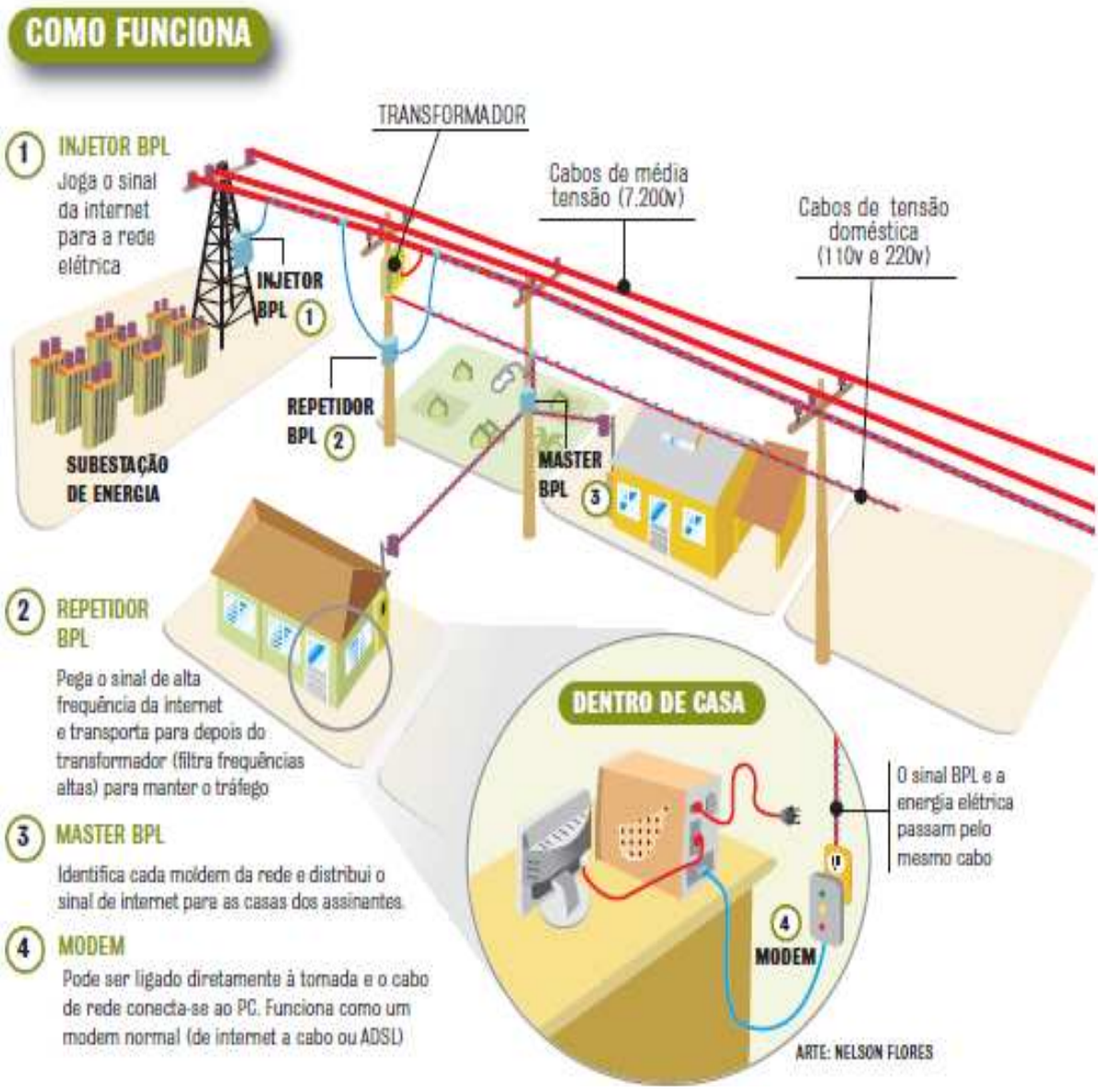


Figura 14: Funcionamento de uma rede BPL

Pelo fato da capa plástica absorver sinais de alta frequência, temos um grande problema quando desejamos manter uma conexão de alta velocidade e com grandes distâncias entre os repetidores BPL. Por isso algumas vezes temos a necessidade de instalar repetidores BPL mesmo que não haja um transformador.

Outro grande problema que encontramos na implantação de redes BPL é o fato de que nem sempre as linhas elétricas encontram-se em condições de suportar tal conexão, pois muitas vezes a infra estrutura é antiga e apresenta muitas perdas elétricas que podem ocasionar perdas dos pacotes.

5.2 CONDIÇÕES DE USO DE RADIOFREQUÊNCIAS POR SISTEMAS BPL

Em 8 de abril de 2009 a ANATEL (Agência Nacional de Telecomunicações) aprovou a resolução de nº 527 que, junto com a resolução de nº 375 aprovada pela ANEEL (Agência Nacional de Energia Elétrica) em 25 de agosto de 2009, define as condições que as prestadoras de serviços de telecomunicações devem cumprir para poder utilizar o sistema de rede elétrica para fornecer serviços de acesso à banda larga no Brasil.

Uma das preocupações da ANATEL é quanto à radiação emitida pelos sistemas BPL tanto em redes de baixa tensão (RBT), quanto em redes de média tensão (RMT). As tabelas 7 e 8 mostram os limites de radiações indesejadas que são aceitos pela ANATEL.

Tabela 7: Limites de radiações indesejadas causadas por sistemas BPL de RBT

Faixa de freqüências (MHz)	Intensidade de campo (microvolt por metro)	Distância da Medida (metro)
1,705-30	30	30
30-50	100	3

Tabela 8: Limites de radiações indesejadas causadas por sistemas BPL de RMT

Faixa de freqüências (MHz)	Intensidade de campo (microvolt por metro)	Distância da Medida (metro)
1,705-30	30	30
30-50	90	10

Além dessa preocupação quanto ao nível de radiação emitidos, a ANATEL impôs as exclusões de algumas faixas de frequências, que podem ser destinadas posteriormente ao Serviço Móvel Aeronáutico, no segmento de espectro compreendido entre 1,705 MHz e 50 MHz. Essas faixas de frequências excluídas podem ser vistas na tabela 9.

Tabela 9: Faixas de radiofrequências em redes de média tensão excluídas

Faixas de Exclusão Faixas de frequências (MHz)
2,754 - 3,025
3,400 - 3,500
4,453 - 4,700
5,420 - 5,680
6,525 - 6,876
6,991 - 7,300
8,815 - 8,965
10,005 - 10,123
11,275 - 11,400
13,260 - 13,360
13,927 - 14,443
17,900 - 17,970
21,000 - 21,450
21,924 - 22,000
28,000 - 29,700

Além dessas faixas de exclusão, dentro das zonas de proteção costeira deverão ser observados os seguintes critérios:

- Na faixa de radiofrequência de 2,1735 – 2,1905 MHz, fica vedada a operação de quaisquer sistema BPL.
- Nas faixas de radiofrequências listadas na tabela 10, os limites de radiação indesejada causada pelos sistemas BPL em Redes de Média Tensão devem estar atenuados a um nível de, pelo menos, 10dB abaixo dos limites especificados nas tabelas 7 e 8.

Tabela 10: Faixas de Radiofrequências relativas à zona de proteção de estações costeiras

Faixas de frequências (MHz)
4,122 - 4,128
4,177 - 4,178
4,207 - 4,208
6,212 - 6,218
6,268 - 6,269
6,312 - 6,313
8,288 - 8,294
8,364 - 8,365
8,376 - 8,377
12,287 - 12,293
12,520 - 12,521
12,577 - 12,578
16,417 - 16,423
16,695 - 16,696
19,680 - 19,681
22,376 - 22,377
26,100 - 26,101

Tabela 11: Coordenadas das Zonas de Proteção de Estações Costeiras

CIDADE	UF	Coordenadas Geográficas	
		LATITUDE	LONGITUDE
Arraial do Cabo	RJ	22S5655	42W0140
Belém	PA	01S2341	48W2927
Belém	PA	01S2752	48W3016
Belém	PA	01S2346	48W2644
Belém	PA	01S2701	48W2918
Brasília	DF	15S4707	47W5130
Brasília	DF	15S5947	47W5356
Cabo Frio	RJ	22S4258	42W0017
Duque de Caxias	RJ	22S4813	43W1727
Itajaí	SC	27S0435	48W4620
Ladário	MS	19S0014	57W5357
Manaus	AM	03S0818	60W0130
Manaus	AM	03S0827	60W0122
Manaus	AM	03S0616	59W5416
Natal	RN	05S4730	35W1313
Natal	RN	05S4732	35W1152
Niterói	RJ	22S5305	43W0758
Parnamirim	RN	05S5155	35W1618
Recife	PE	08S0604	35W0118
Rio de Janeiro	RJ	22S4645	43W0916
Rio de Janeiro	RJ	22S5226	43W0806
Rio de Janeiro	RJ	22S5357	43W1037
Rio de Janeiro	RJ	22S4937	43W1106
Rio de Janeiro	RJ	22S5451	43W1701
Rio de Janeiro	RJ	23S0000	43W3622
Rio Grande	RS	32S0150	52W0454
Rio Grande	RS	32S0824	52W0616
Rio Grande	RS	32S0202	52W0420
Rio Grande	RS	32S0823	52W0625
Rio Grande	RS	32S0349	52W0837
Salvador	BA	12S4830	38W2947
Salvador	BA	12S5827	38W3055
São Gonçalo	RJ	22S5045	43W0608
São Pedro da Aldeia	RJ	22S4927	42W0532

Além de ter que seguir essas resoluções, para se ter uma rede BPL funcionando perfeitamente, todos os equipamentos utilizados na formação dessa rede devem seguir as normas impostas pelo padrão P1901 criado pelo IEEE que define os padrões de controle de acesso ao meio e camada física que esses equipamentos devem seguir.

5.3 MONITORAMENTO DE ENERGIA ATRAVÉS DO BPL

Atualmente, quando ocorre algum problema na rede elétrica, como um transformador estourado ou cabos partidos, a companhia de eletricidade conta com a ligação de reclamação de um cliente para abrir uma ordem de chamado e assim poder resolver o problema.

O monitoramento de energia através do PLC é feito através do uso de *grids* inteligentes, que têm a função de monitorar toda a extensão da fiação da rede elétrica, acionando diretamente a central caso haja alguma falha de energia ou problemas em um transformador instalado. Esses *grids* informam com precisão o local onde ocorreu esta falha, permitindo que a companhia de eletricidade consiga descobrir a existência de problemas na rede elétrica em tempo real, e fazendo atendimento mais rápido e eficaz ao cliente.

Os *grids* inteligentes também conseguem reduzir as perdas de energia na rede elétrica, pois ele identifica cabos e transformadores com perdas.

Através do monitoramento da rede elétrica fica mais fácil a companhia de eletricidade descobrir a existência de *gatos,* que é o roubo de energia elétrica, em sua rede, gerando uma grande economia para essa companhia.

Outra vantagem que também é estudada, devido à facilidade de monitoramento gerada pela tecnologia PLC, é a possibilidade de dar descontos nas tarifas de energia cobradas em determinados horários, o que pode fazer com que haja uma maior

economia de energia no país inteiro. É uma alternativa bastante interessante ao governo que tem feito um grande esforço para obter um melhor uso da eletricidade, como a realização do horário de verão, por exemplo.

Futuramente, esse monitoramento tende a ultrapassar as barreiras da concessionária de energia, trazendo maiores vantagens para o usuário final, como por exemplo a possibilidade de acompanhar o gasto que ele está tendo, de ligar ou desligar um aparelho, uma iluminação ou qualquer coisa ligada à rede elétrica através da internet.

6 CONCLUSÃO

A tecnologia PLC vem se concretizando como uma grande aposta para levar telefonia e acesso por meio de banda larga através das redes de distribuições de energia, principalmente para locais distantes dos grandes centros urbanos, trazendo conhecimento, empregos e principalmente desenvolvimento para essas regiões.

Após anos de estudo para resolver problemas de interferência causados pelo meio elétrico, esta tecnologia já está regulamentada e em testes por diversas companhias elétricas, que devem usá-la dentro em breve como uma nova fonte de renda, o que é muito bom para os consumidores pois aumentará a oferta para serviços de telefonia e banda larga.

O uso de *grids* inteligentes também é um grande avanço científico, pois melhora a qualidade do serviço de fornecimento de eletricidade prestado, reduzindo perdas elétricas, e trazendo um enorme avanço tecnológico para eletrodomésticos e tarefas diárias.

Além disso, pode-se utilizá-la como uma opção para nossas redes locais (LANs), pois os aparelhos PLC já estão sendo comercializados com preços competitivos, e com a grande vantagem de não necessitarem de uma nova infra-estrutura de cabeamento.

7 REFERÊNCIAS BIBLIOGRÁFICAS

[1] http://www.malima.com.br/article_read.asp?id=219 acessado em 20,21 e 27 de outubro de 2007.

[2] http://pt.wikipedia.org acessado em 20,21 e 27 de outubro de 2007.

[3] http://www.teleco.com.br/tutoriais/tutorialplc/ acessado em 20,21 e 27 de outubro, 3, 11, e 17 de novembro de 2007.

[4] http://www.vivaolinux.com.br/artigo/Redes-PLC acessado em 3, 11, e 17 de novembro de 2007; 05, 06 e 07 de março de 2010.

[5] http://www.smartsec.com.br/plc.html acessado em 20,21 e 21 de outubro, 3, 11, e 17 de novembro de 2007; 05, 06 e 07 de março de 2010.

[6] http://informatica.hsw.uol.com.br/comunicacao-por-fiacao-eletrica1.htm acessado em 20,21 e 21 de outubro, 3, 11, e 17 de novembro de 2007; 05, 06 e 07 de março de 2010.

[7] http://www.gta.ufrj.br/grad/07_1/plc/plc_apres.ppt acessado em 3, 11, e 17 de novembro de 2007; 05, 06, 10, e 13 de março de 2010.

[8] http://www.pee.ufrj.br/teses/?Resumo=2005050401 acessado em 3, 11, e 17 de novembro de 2007; 05, 06, 10, e 13 de março de 2010.

[9] http://www.hd-plc.org/english/Default.aspx acessado em Novembro de 2007, e Março de 2010

[10] http://www.ntia.doc.gov/osmhome/reports/2007/bpl2007.html acessado em Março de 2010

[11] http://www.currentgroup.com acessado em Outubro e Novembro de 2007, e em Março de 2010

[12] http://www.gta.ufrj.br/grad/00_2/ieee/CSMA.htm acessado em Abril de 2010

[13] http://www.homeplug.org acessado em Março e Abril de 2010

[14] TANENBAUM, A.S. **Redes de Computadores. 4.ed.** 945p.

[15] BRASIL. Resolução nº 527, de 8 de abril de 2009. Aprova o Regulamento sobre Condições de Uso de Radiofrequências por Sistemas de Banda Larga por meio de Redes de Energia Elétrica. **Agência Nacional de Telecomunicações.** Brasília, DF. Disponível em http://www.ptt-radio.qsl.br/Documentos/Res%20527%202009.pdf. acessado em Março e Abril de 2010

[16] BRASIL. Resolução Normativa nº 334, de 21 de outubro de 2008. Regulamenta o art. 3º, inciso XIII, da Lei nº 9427, de 26 de dezembro de 1996, o qual trata dos controles prévio e a *posteriori* sobre atos e negócios jurídicos entre as concessionárias, permissionárias e autorizadas e suas partes relacionadas. **Agência Nacional de Energia Elétrica.** Brasília, DF. Disponível em http://www.aneel.gov.br/cedoc/ren2008334.pdf acessado em Abril de 2010

[17] BRASIL. Resolução Normativa nº 375, de 25 de agosto de 2009. Regulamenta o a utilização das instalações de distribuição de energia elétrica como meio de transporte para comunicação digital ou analógica de sinais. **Agência Nacional de Energia Elétrica.** Brasília, DF. Disponível em http://www.aneel.gov.br/cedoc/ren2009375.pdf acessado em Abril de 2010

[18] USA. Resolução Normativa FCC 09-60, de 16 de julho de 2009. Regras para dispositivos e sistemas BPL. Federal Communications Commission. Washington, D.C. Disponível em http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-60A1.doc acessado em Março e Abril de 2010